STATE OF GEORGIA
COUNTY OF HENRY
CITY OF STOCKBRIDGE

RESOLUTION R15-635

A RESOLUTION AUTHORIZING CERTAIN AMENDMENTS TO THE PERSONNEL MANUAL; AUTHORIZING THE CITY CLERK TO ATTEST SIGNATURES AND AFFIX THE OFFICIAL SEAL OF THE CITY, AS NECESSARY; REPEALING INCONSISTENT RESOLUTIONS; PROVIDING FOR AN EFFECTIVE DATE; AND FOR OTHER PURPOSES.

WHEREAS, the City of Stockbridge ("City") is a municipal corporation located within Henry County, Georgia duly organized and existing under the laws of the State of Georgia and is charged with providing public services to residents located within the corporate limits of the City; and

WHEREAS, the City finds it necessary to amend certain provisions in the Personnel Policy and Procedure of the City in order to provide for the enhanced protection of confidential information to include criminal background information and fingerprinting information.

THEREFORE, IT IS NOW RESOLVED BY THE CITY COUNCIL OF THE CITY OF STOCKBRIDGE, GEORGIA, AS FOLLOWS:

1. **Approval of Execution.** The City hereby approves the amendments to the Personnel Policy and Procedures attached hereto as Exhibit A. All other policies and regulations of the City previously in existence which relate to the Personnel Policy and Procedures shall remain in full force and effect.

2. **Documents.** The City Clerk is authorized to execute, attest to, and seal any documents which may be necessary to effectuate the amendment, subject to approval as to form by the City Attorney.

3. **Severability.** To the extent any portion of this Resolution is declared to be invalid, unenforceable or non-binding, that shall not affect the remaining portions of this Resolution.

4. **Repeal of Conflicting Provisions.** All City resolutions are hereby repealed to the extent they are inconsistent with this Resolution.

5. **Effective Date.** This Resolution shall be effective on the date of its approval by the City Council and Mayor as provided in the City Charter.

SO BE IT RESOLVED this 9th day of March 2015.

Alphonso Thomas

ALPHONSO THOMAS, Mayor Pro Tem

ATTEST:

Vanessa Holiday

VANESSA HOLIDAY, City Clerk (SEAL)

APPROVED AS TO FORM:

MICHAEL WILLIAMS, City Attorney

SEAL

EXHIBIT A

AMENDMENTS TO PERSONNEL MANUAL

NATURAL OR MAN MADE DISASTERS

In the event of a natural or man-made disaster, the LASO shall have the responsibility of ensuring that the records maintained by the Stockbridge Occupational Tax Office (OTO) are secured and not in danger of being damaged or destroyed.

In the event that the OTO records are not secured or have been damaged and/or destroyed, the LASO shall make immediate notification to the City Manager or City Clerk and GCIC and advise them of the situation.

The LASO shall be responsible for taking the necessary steps to ensure that all records are secured on site or that said records are removed to another location where they can be secured until such time that they can be returned and secured within the Stockbridge Occupational Tax Office.

COMPLAINCE WITH GCIC RULES AND GCIC CJIS SECURITY POLICY

The use and operation of any computer, telephonic or electronic device which enables Stockbridge Occupational Tax Office personnel to interact with any or all parts or portions of the Georgia Crime Information Center will be in strict compliance with the operational rules established by the GCIC Council and the GCIC Security Policy.

Occupational Tax Office personnel who are found in violation of the rules governing the use of the GCIC system or of the GCIC CJIS Security Policy will be subject to the established Disciplinary Policy of the City of Stockbridge, which may include, but not limited to suspension or termination.

Additionally, any Occupational Tax Office personnel who have been found to be in violation of the GCIC Rules or GCIC CJIS Security Policy may be subject to criminal prosecution.

City of Stockbridge

4640 North Henry Boulevard
Stockbridge, Georgia 30281
770-389-7900

STANDARD OPERATING PROCEDURES

Subject: Georgia Crime Information Center (GCIC)/National Crime Information Center (NCIC) Disciplinary Action for Violations

Effective Date: 03/09/2015

Purpose:

The purpose of this policy is to establish guidelines for disciplinary action in regards to violations concerning the Georgia Crime Information Center state system/National Crime Information Center and information obtained thereof.

This policy applies to all agency employees with access, to include physical and logical access, to GCIC/NCIC. This policy will establish guidelines for disciplinary action to be taken in regard to the usage of the GCIC/NCIC and information obtained thereof.

All employees are required to follow the policies, rules and procedures set forth by GCIC, NCIC, FBI CJIS Security Policy, and the laws of the State of Georgia.

A. The following disciplinary action will be taken for general working errors that involve violations which are determined to be accidental errors or errors made due to the need of additional training. The severity of the error will be evaluated by the Terminal Agency Coordinator. This is a general guideline and its use will be determined by the Terminal Agency Coordinator, Administrative Head, and/or Agency Head.

1st offense (for less severe errors) Verbal Warning- additional training
1st offense or 2nd offense (determined by the severity of error) – written reprimand (additional training)
3rd offense – written reprimand with possible suspension or termination – extensive additional training
4th offense – employment termination

B. For deliberate violations and/or misuse of GCIC/NCIC or information obtained thereof;

1st offense – immediate termination and possible criminal prosecution

City of Stockbridge
4640 North Henry Boulevard
Stockbridge, Georgia 30281
770-389-7900

MEDIA PROTECTION

SECTION 10

10.0 Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

10.1 Media Storage and Access

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

10.2 Media Transport

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

10.3 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

10.4 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

10.5 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

10.6 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

10.7 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 12 – A Local Police Department's Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor's vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentially of the police department's data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor's vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

SECTION 11

11.0 Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

11.1 Physically Secure Location

A physically secure location is a facility, a police vehicle, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof. Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

11.2 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

11.3 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

11.4 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

11.5 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

11.6 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

11.7 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

11.8 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

11.9 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

11.10 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.

2. Lock the area, room, or storage container when unattended.

3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

11.11 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by dispatchers, officers, and detectives. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

SECTION 12

12.0 System and Communication Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

12.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.

2. Block outside traffic that claims to be from within the agency.

3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

12.2 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.

2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.4 for guidance on personal firewalls.

4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.

5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

12.3 Encryption

Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

1. Encryption shall be a minimum of 128 bit.

2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption). EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.

3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).

   a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:

i. Be at least 10 characters

ii. Not be a dictionary word.

iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.

iv. Be changed when previously authorized personnel no longer require access.

b) Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

4. When encryption is employed the cryptographic module used shall be certified to meet FIPS 140-2 standards. Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete. Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.

5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

a) Include authorization by a supervisor or a responsible official.

b) Be accomplished by a secure process that verifies the identity of the certificate holder.
c) Ensure the certificate is issued to the intended party.

12.4 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools. The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.

2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.

3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

12.5 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.

2. Change the default administrative password on the IP phones and VoIP switches.

3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

12.6 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146),as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

12.7 Facsimile Transmission of CJI

CJI transmitted via facsimile is exempt from encryption requirements.

12.8 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

12.9 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.

3. Different instances of the operating system.

4. Different network addresses.

5. Other methods approved by the FBI CJIS ISO dividing the

12.10 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.

2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.

3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally.

4. Device drivers that are "critical" shall be contained within a separate guest.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.

2. Implement IDS and IPS monitoring within the virtual machine environment.

3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.

4. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization

SECTION 13

13.0 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.

2. Rollback capabilities when installing patches, updates, etc.

3. Automatic updates without individual user intervention.

4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

13.1 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.